



WASHINGTON, D.C. 20301

POLICY

3 November 1982

MEMORANDUM FOR THE CHAIRMAN, DCI SECURITY COMMITTEE

SUBJECT: Policy on Unauthorized Disclosures and on Damage Assessments

Reference is made to your memorandum, SECOM-D-344, of 28 October 1982, which requested concurrences or comments concerning the Unauthorized Disclosures Investigations Subcommittee (UDIS) reports on subject topics.

Concerning the National Policy on Unauthorized Disclosures, we continue to support option two as defined in the paper, which would allow some progress concerning the acceptable provisions of the Willard Report. You were correct in recounting the Security Committee's agreement that there is no need for another iteration of the Willard Report, and that the paper of the UDIS can serve the purpose of the CIA Member in responding to the IG/CM if he so desires. It would seem to be the option of the Director of Central Intelligence, politically, as to whether, or when, he should again ask Judge Clark to complete his evaluation of the Willard Report and provide recommendations to the President.

Concerning the paper, Points for Consideration Relative to A National Policy on Damage Assessments, we see no need for national level guidance to trigger investigations, generally. Agency heads responsible for protecting their information, both under the basic theory of the E.O. 12356 concerning the protection of national security information, and on the basic theory of command responsibility, if you will, are in the best position to determine whether an investigation is needed, and, if so, to what extent. If there is impact beyond the Agency immediately victimized, requests will certainly go to other agencies to take action, or to assist appropriately, as is done now.

Concerning quality control, agency heads have a management responsibility in this regard too, and it would seem to be a bit intrusive for an outside organization or agency to be dictating control practices to individual agencies. It impinges a bit on the authorities of an Agency head to manage his affairs, one would think. From the standpoint of the Department of Defense, such external imposition of requirements is unnecessary in that we have a formal, well-established process of monitorship and assistance from the Departmental level through Defense Agencies and the Military Departments to ensure that such matters receive proper attention.

Assessment implementation further intrudes into the prerogatives of the Agency head, it would seem. All managers have inspection and review responsibilities under the basic national program for the protection of national security

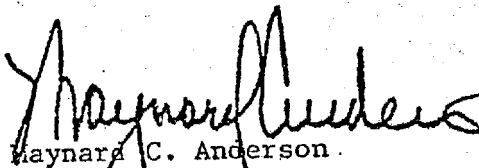
information as well as for all special and particular programs in which they participate. Suffice it to say that any guidance in this regard should be limited to the requirement that Agency heads or program managers should ensure implementation of corrective action.

Sharing of information has some value from a lessons-learned perspective. Like the Security Committee Study on Harrassments and Provocations, the Defense Industrial Security Newsletter, and the USAF Newsletter cited, there may be some future value in sharing experiences, treatment of problems, and determination of solutions in this arena. It is recommended that the Security Education and Training Subcommittee be charged to examine this suggestion.

Before substantive comments either for or against the establishment of a data base can be offered, there is a need to see a more detailed proposal to understand whether the value of the data base is worth the effort and expense. One problem is apparent immediately - despite any and all assurances of safeguards, there are many program managers who will not share information concerning leaks of their information with the managers of such a data base because the information concerns research and development programs on the leading edge of technology, or information concerning sensitive sources and methods. Additionally, the information put into the data base will have to be shared with everyone who needs it - and that might be a relatively large audience - to be effective. The establishment of a data base has good and valid objectives despite doubts that it will identify or isolate leakers. It is recommended, however, that the proponents construct and submit a plan to include data elements to be included, format, safeguards, objectives and potential costs for our consideration so that we can make intelligence judgements about its potential value.

The Department of Defense publishes DoD 5200.1-R in implementation of E.O. 12356 and ISOO Directive No. 1.

For your information, in case you had not seen it, I enclose a recent article entitled "Plugging Leaks", from the Army Times issue of 25 October 1982.



Maynard C. Anderson
Director
Security Plans and Programs